TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
04/20/2017

SUBJECT:
Multiple Vulnerabilities in Google Chrome Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could result in remote code execution. Google Chrome is a web browser used to access the Internet. These vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted web page. Successful exploitation of these vulnerabilities could allow an attacker to execute remote code in the context of the browser, obtain sensitive information, bypass security restrictions, or cause denial-of-service conditions.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
* Google Chrome prior to 58.0.3029.81

RISK:
Government:
* Large and medium government entities: **High**
* Small government entities: **Medium**
Businesses:
* Large and medium business entities: **High**
* Small business entities: **Medium**
Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could result in remote code execution. These vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted web page. Details of the vulnerabilities are as follows:

* Type confusion in PDFium (CVE-2017-5057).
* Heap use after free in Print Preview (CVE-2017-5058).
* Type confusion in Blink (CVE-2017-5059).
* URL spoofing in Omnibox (CVE-2017-5060, CVE-2017-5061, CVE-2017-5067).
* Use after free in Chrome Apps (CVE-2017-5062).

- Heap overflow in Skia (CVE-2017-5063).
- Use after free in Blink (CVE-2017-5064).
- Incorrect UI in Blink (CVE-2017-5065).
- Incorrect signature handing in Networking (CVE-2017-5066).
- Cross-origin bypass in Blink (CVE-2017-5069).

Successful exploitation of these vulnerabilities could allow an attacker to execute remote code in the context of the browser, obtain sensitive information, bypass security restrictions, or cause denial-of-service conditions.

RECOMMENDATIONS:
The following actions should be taken:
- Apply appropriate patches provided by Google to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Google:
https://chromereleases.googleblog.com/2017/04/stable-channel-update-for-desktop.html

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5057
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5058
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5059
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5060
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5061
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5062
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5063
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5064
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5065
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5066
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5067
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5069